PIERCE O'DONNELL (SBN 081298)
PODonnell@GreenbergGlusker.com
TIMOTHY J. TOOHEY (SBN 140117)
TToohey@GreenbergGlusker.com
PAUL BLECHNER (SBN159514)
PBlechner@GreenbergGlusker.com
GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
2049 Century Park East, Suite 2600
Los Angeles, California 90067-4590
Telephone: 310.553.3610
Fax: 310.553.0687

Attorneys for Plaintiff
MICHAEL TERPIN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

MICHAEL TERPIN,

Plaintiff,

v.

AT&T MOBILITY, LLC; and DOES 1-25,

Defendants.

Case No. 2:18-cv-06975-ODW-KS

PLAINTIFF'S OPPOSITION TO MOTION TO DISMISS THE SECOND AMENDED COMPLAINT OF DEFENDANT AT&T MOBILITY, LLC.

[Fed. R. Civ. Proc. 12(b)(6)]

Assigned To:
Honorable Otis D. Wright II

Hearing: May 4, 2020
Time: 1:30 p.m.
Dept./Place: 350 West 1st Street
5th Floor, Courtroom 5D
Los Angeles, CA 90012

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

TABLE OF CONTENTS

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

TABLE OF AUTHORITIES

CASES

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

STATUTES

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

I. INTRODUCTION

The motion to dismiss ("Motion") Plaintiff's Second Amended Complaint ("SAC") of Defendant AT&T Mobility, LLC ("Defendant" or "AT&T") inappropriately distorts the allegations made by Plaintiff Michael Terpin ("Plaintiff" or "Mr. Terpin") in an improper attempt to dismiss Mr. Terpin's fraud and punitive damages claims. The Motion should be denied.

First, Mr. Terpin has properly plead his third and fourth claims for relief for deceit by concealment and misrepresentation. AT&T virtually ignores the fact that Mr. Terpin has alleged that its representatives made *specific false representations* to Mr. Terpin after the first SIM swap on June 11, 2017 that were intended to induce him to continue being an AT&T customer, upon which he relied (to his very considerable detriment) and that are more than adequate to support his claims for deceit by concealment and misrepresentation. Moreover, one of AT&T's primary arguments—that Mr. Terpin has not alleged more facts to support his fraud claims—is belied by the fact that AT&T alone is in possession of such facts and has delayed discovery that will reveal additional facts by bringing three successive motions to dismiss since this action was filed in August 2018.

Second, Mr. Terpin has properly plead punitive damages. AT&T's attempt to strike the punitive damages claim similarly rests on a seemingly willful distortion of Plaintiff's allegations regarding AT&T's involvement in the SIM swaps alleged in the SAC. Mr. Terpin's primary argument is that AT&T through its corporate officers and managing directors created an inadequate "security" system that allowed its employees and contractors to bypass controls to implement SIM swaps (either on their own or in conjunction with hackers from whom they accepted small bribes). In other words, Mr. Terpin is not "focus[ing]" (as AT&T alleges) on Jahmil Smith, but rather on the fact that AT&T knowingly and with deliberate disregard to the privacy of its customers put in place and maintained a highly

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

inadequate security system that it knew could not prevent its own employees from facilitating SIM swaps. *See* AT&T Motion to Dismiss FAC ("Motion") at 8 n.3.

Further, especially in light of AT&T's repeated assertions that Mr. Smith was *not an AT&T* employee[1], AT&T's extensive reliance on cases under California Civil Code Section 3294(b), which pertain to the ratification of acts of low-level employees, is inapposite. Mr. Terpin has adequately alleged a basis for a claim for punitive damages in the context of AT&T's knowledge and obligations to protect customer information, including its obligations to monitor and supervise its employees under a prior consent decree from the Federal Communications Commission ("FCC") that dealt with precisely that issue. Mr. Terpin has further alleged that AT&T and its officers and managing agents, including AT&T's Chief Compliance Officer and head of security, knew of the inadequacy of AT&T's security measures and deliberately disregarded and violated the rights of its customers, including Mr. Terpin, all while continuing to falsely assure customers that they could obtain a higher level of security by upgrading to a six-digit code. As properly alleged in the SAC, AT&T is subject to punitive damages for Mr. Terpin's fraud and tort claims and AT&T's motion to strike such damages should be denied.

II. ARGUMENT

A. Mr. Terpin Has Appropriately Alleged Deceit by Concealment.

1. Mr. Terpin alleges that AT&T deceived him after the June 11, 2017 hack.

In his third claim for relief, Mr. Terpin alleges that AT&T knew its data security system was grossly inadequate and that its employees could readily bypass

[1] AT&T has repeatedly made this assertion in its motions to dismiss, despite the irrelevance of such factual assertions for such motion (defendant is bound to accept the plaintiff's allegations as true). *See*, *e.g.*, *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001) (defendant's factual assertions are irrelevant to a motion to dismiss).

whatever protections it purported to give. SAC ¶¶ 143-145. This claim is further substantiated elsewhere in the SAC. For example, in Paragraph 78, Mr. Terpin alleges that an AT&T employee confirmed in an August 3, 2018 article in *Motherboard*, that "*the* [AT&T] *system is designed so that some employees have the ability to override security features such as the phone passcode that AT&T (and other companies) now require when porting numbers*. 'From there the passcode can be changed,' the employee said in an online chat, referring to a customer information portal that they showed *Motherboard*. 'With a fresh passcode the number can be ported out with no hang ups.'" (Emphasis added.)

After Mr. Terpin's initial SIM swap, he went on June 11, 2017 to an AT&T store in Puerto Rico to ask what additional security could be implemented on his account to prevent future hacks. SAC ¶ 88. As alleged in the SAC, "Mr. Terpin explained to AT&T that he had been hacked and that the hackers had stolen a substantial amount of money from him. Mr. Terpin expressed concern about AT&T's ineffective security protections and asked how he could protect the security of his phone number and account against future unauthorized access, including hackers attempting to perpetrate SIM swap fraud." *Id.*

As further alleged in the SAC:

> [i]n response to Mr. Terpin's request for greater security for his account and in order to induce Mr. Terpin to continue as an AT&T customer, AT&T promised that it would place his account on a "higher security level" with "special protection." AT&T told Mr. Terpin that this "higher security level" would require anyone accessing or changing Mr. Terpin's account to provide a six-digit passcode to AT&T to access or change the account. Anyone requesting AT&T to transfer Mr. Terpin's telephone number to another phone must provide the code. AT&T promised Mr. Terpin at this meeting that the higher

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

> security that it was placing on his account, which it also called "high risk" or "celebrity" protection, would ensure that Mr. Terpin's account was much less likely to be subject to SIM swap fraud. AT&T further told Mr. Terpin that the implementation of the increased security measures would prevent Mr. Terpin's number from being moved to another phone without Mr. Terpin's explicit permission, because no one other than Mr. Terpin and his wife would know the secret code. AT&T made all of these promises to convince Mr. Terpin to continue to be an AT&T customer.

Id. *See also* SAC ¶¶ 143, 148, 150.

In inducing Mr. Terpin to stay with AT&T by promising that the "high risk" protection allegedly afforded by the additional six-digit Code would increase the security of his account, AT&T did not disclose that the additional security was worthless or ineffective because it could easily be bypassed or ignored by AT&T employees. ¶ 144. Specifically, AT&T "knew that its data security measures were grossly inadequate, that its employees and agents could readily bypass the procedures, that its employees actively cooperated with hackers and thieves, and that it was incapable of living up to its commitments to consumers, including to Mr. Terpin, under state and federal law, as well as under its own Privacy Policy, to protect his Personal Information, including CPI and CPNI." SAC ¶ 143. AT&T made these false promises to induce Mr. Terpin to remain a customer. *Id.* Mr. Terpin believed AT&T's promises and remained an AT&T customer. *Id.* ¶¶ 143, 151.

The SAC also alleges that AT&T made the following false statements and/or omissions to Mr. Terpin:

(1) In June 2017, after the initial SIM swap, AT&T representatives encouraged Mr. Terpin to adopt additional security measures (adding a

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

six digit code) without telling Mr. Terpin that such security measures could readily be evaded or bypassed by AT&T employees acting in concert with individuals perpetrating SIM swap fraud;

(2) at all times herein relevant prior to the second SIM swap in January 2018, AT&T concealed the fact that its employees frequently acted in concert with individuals perpetrating SIM swap fraud to provide such individuals with personal information about its mobile users;

(3) at all times herein relevant prior to the second SIM swap in January 2018, AT&T concealed the fact that its employees frequently acted in concert with individuals perpetrating SIM swap fraud to provide such individuals with direct access to their customers' accounts, which enabled such individuals to intercept 2FA messages to customers; and

(4) because of the inadequacies of AT&T's security measures and the active participation of its employees in SIM swaps that AT&T's promises in its Privacy Policy had no value.

SAC ¶ 144.

2. AT&T Had a Duty to Disclose Material Facts.

AT&T alleges that Plaintiff's Third Claim for Deceit by Concealment should be dismissed because defendant did not have a legal duty to disclose a material fact. AT&T's argument is incorrect because three of the four circumstances set forth in *Hodson v. Mars, Inc.*, 891 F.3d 857, 862 (9th Cir. 2018), which it cites, existed in this case.

First, a duty arose because AT&T in fact had "exclusive knowledge of material facts" relating to its security system. Mr. Terpin had no way of knowing that the additional security precautions that AT&T was urging were not adequate. He accepted the affirmative statements that AT&T made after the June 11, 2017 SIM swap and did not realize AT&T was hiding and concealing the true facts. SAC ¶¶ 92, 143. Although Mr. Terpin was knowledgeable about cryptocurrency—

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

the SAC does not allege that he was an expert on security measures of telecommunications providers, *id*. ¶ 18, nor is such an inference logical. Indeed, as the SAC alleges, Mr. Terpin was only contacted by other victims of SIM swaps *after* he filed the initial complaint in this action. *See* SAC ¶ 14 ("[*s*]*ince the hack to Mr. Terpin has occurred and this lawsuit has been filed*, he has been contacted by more than 50 SIM swap victims of AT&T, including many who had cryptocurrency stolen under nearly identical circumstances") (emphasis added).[2]

By contrast, AT&T is one of the world's largest corporations and it and its Chief Security Officer Bill O'Hern and Chief Compliance officer David Huntley may fairly be presumed to have profound and superior knowledge about its security system. *Id*. ¶ 75. Moreover, AT&T is legally required by the Federal Communications Act ("FCA"), 47 U.S.C. §§ 206, 222 and an ongoing FCC Consent Degree to protect its customers' personal information, including protecting it from being improperly accessed by its own employees. *Id*. ¶¶ 39-46, 51. Under these circumstances AT&T undoubtedly had the "exclusive knowledge" sufficient to give rise to a duty to speak

Secondly, AT&T also had a duty under *Hodson* to disclose material facts to Mr. Terpin because it actively concealed material facts from Mr. Terpin. Specifically, AT&T told Mr. Terpin on June 13, 2017 that he would be protected against future SIM swaps by using the "higher" security afforded by a six digit code but actively concealed the fact this security could be overridden or ignored by AT&T employees. *See* SAC ¶¶ 11, 13, 77-79, 83, 89-94. AT&T's concealment is indeed an "affirmative act" directed to Mr. Terpin in which AT&T hid or concealed its imperfect security. *See Czuchaj v. Conair Corp.*, 2014 WL 1664235, at * 6 (S.D.Cal. April 18, 2014). AT&T's active concealment consisted of its intentional

[2] Similarly, all of the SIM swaps referenced in the SAC occurred *after Mr. Terpin's* SIM swap. *See* SAC ¶¶ 60-82. The only SIM Swap which is referenced in the SAC that occurred *before* the January 2018 hack was that experienced by Mr. Terpin on June 11, 2017. *See* SAC ¶¶ 88-89.

act in seeking to retain Mr. Terpin as a customer.

AT&T's statements after the June 11, 2017 are "partial representations" by AT&T that were accompanied by "concealment of material facts" that also gave rise to a duty to speak. *See Hodson* at 862 (quoted in the Motion at p. 5). The "partial representations" are AT&T's statements regarding the efficacy of the six-digit code. The "concealment" is AT&T's concealment of the fact that employees could easily evade or bypass these protections, which in turn reveals the fallacy of the assurances of higher security as a result of using the six-digit code. AT&T's concealment certainly involves facts that would have "materially qualif[ied] the facts disclosed or which render [AT&T's] disclosure likely to mislead." *Herron v. Best Buy Co. Inc.*, 924 F. Supp. 2d 1161, 1177 (E.D.Cal. 2013). *See* SAC ¶ 161 ("Mr. Terpin would not have agreed to continue to use and pay for AT&T's services if he had known that the additional security protection was ineffective and that AT&T's other security measures were not as secure as represented by AT&T. . . .")

AT&T is thus incorrect in stating that the "gravamen" of the SAC is the inadequacy of AT&T's security system in and of itself. Mr. Terpin has multiple claims and these concealment claims are grounded in the allegations that the specific statements about heightened additional security, which were made to him by AT&T after the June 11, 2017 hack, were inadequate and that AT&T made material omissions regarding those statements to hide the inadequacy of its security measures.

Mr. Terpin further provides adequate context for his allegations regarding the falsity and incompleteness of AT&T's promises regarding the "higher level" six-digit security. SAC ¶¶ 89-90. Based on information and investigations obtained by Mr. Terpin, including information after his initial complaint was filed, Mr. Terpin has alleged that AT&T employees frequently bypass or ignore its vaunted security systems, including the additional code, because such security could be easily

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

overridden. For example, Mr. Terpin includes in his allegations statements by the Santa Clara County REACT task force that telecommunication providers' security is highly inadequate in preventing SIM fraud. SAC ¶ 74 ("someone needs to light a fire under some folks [at the telecommunications providers] to get these protections [to prevent SIM swap fraud] in place"). He further alleges that according to an AT&T employee quoted in the August 3, 2018 *Motherboard* article that AT&T employees can override security features including "the phone passcode that AT&T (and other companies) now require when porting numbers" (SAC ¶ 78). Mr. Terpin's allegations thus provide more than adequate context for his allegations that AT&T had a duty to disclose material facts to him when he met with AT&T after the June 11, 2017 SIM swap.

AT&T's argument that it disclosed (generally) in its Privacy Policy that it does not "guarantee" security does not mean either that it had no duty to disclose additional facts regarding security or provide AT&T from immunity particularly as regards to the "higher level" security it convinced Mr. Terpin to place on his account. The unremarkable statement that AT&T cannot "guarantee" security in no way obviates Mr. Terpin's allegation that he relied on the statements made regarding a specific security measure that he was urged to place on his account, particularly because AT&T told him that "anyone accessing or changing Mr. Terpin's account [would have] to provide a six-digit passcode to AT&T." SAC ¶ 89.[3] Unlike the cases cited in the Motion at p. 8, AT&T's "warning" was highly general and AT&T certainly did not reiterate the warning when it fought to keep Mr. Terpin's business by encouraging specific implementation of the "higher level"

[3] AT&T's anodyne statement that it could not "guarantee" perfect security would hardly have alerted Mr. Terpin to the fact that AT&T did not even have rudimentary security to protect its own systems from misuse or that its employees could readily evade or override its security measures. *See* SAC ¶ 58. *See also* ¶ 78 (AT&T employee cited to fact that AT&T employees could evade or override security measures, including the "phone passcode that AT&T (and other companies) now require when porting numbers."

security through the six-digit code. This is therefore not a situation like that in *Riggins v. Ortho McNeil Pharm. Inc.*, 51 F. Supp. 3d 708, 712 (N.D. Ohio 2014), where the defendant disclosed dangers when it sold a product. Nor did AT&T in fact "actually disclose" any information regarding the defects of the additional security measures when it made statements regarding the "higher level" six-digit code security on June 13, 2017. In contrast to *Clayton v. Landsing Pac. Fund, Inc.*, 2002 WL 1058247, at *6 (N.D.Cal. May 9, 2002), *aff'd*, 56 F. App'x 379 (9th Cir. 2003), at the time the representations were made by AT&T to Mr. Terpin, information regarding the inefficacy of the six-digit code was not readily found in the market. Mr. Terpin's allegations regarding the ease by which employees could evade the security is based on information obtained after he was SIM swapped.

3. Mr. Terpin Has Adequately Plead that he was Unaware of Concealed Material Facts.

AT&T is incorrect that Mr. Terpin has not adequately plead he was aware of the concealed material facts. In the SAC, Mr. Terpin specifically alleges that he was unaware that AT&T concealed that the additional security he was promised after the June 11, 2017 hack (i.e., the six-digit passcode) was inadequate. SAC ¶ 92. Moreover, he specifically alleges that if he had been aware that the additional security was inadequate, that he would have left AT&T as his mobile carrier. *Id.*

It is risible for AT&T to claim that Mr. Terpin would have known that AT&T's six-digit code could be overridden or evaded by AT&T employees simply by virtue of his involvement in cryptocurrency. Motion, p. 9. Moreover, as AT&T itself acknowledges, Mr. Terpin was only contacted by other victims of AT&T's inadequate security practices *after* he filed his complaint in this action so that information could not have put him on guard regarding AT&T's fraud. Moreover, for AT&T to claim that because Mr. Terpin had been victimized in the first SIM swap that he should have known about the inadequacies of AT&T's security is astonishingly obtuse. Having been SIM swapped, Mr. Terpin was of course aware

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

of the practice. This is why he asked for (and was promised by AT&T) additional security. In the event, AT&T did not disclose when he met with AT&T that the additional security measures were worthless.

B. Mr. Terpin Has Adequately Plead His Fourth Claim for Relief for Misrepresentation.

1. Mr. Terpin Adequately Alleges Reliance.

In his misrepresentation claim, Mr. Terpin alleges that "separate" from representations and false promises made by AT&T in its Code of Business Conduct and other documents that "an AT&T employee made specific promises to Mr. Terpin after the June 11, 2017 hack regarding the security protection that would be given to Mr. Terpin's personal information by adding a six-digit security code on the account. The AT&T employee did so in order to persuade Mr. Terpin not to cancel his AT&T service." SAC ¶ 159. Mr. Terpin further alleges that "AT&T intended that Mr. Terpin rely on their representations and promises, including those made after the June 11, 2017 hack, as it knew that Mr. Terpin would not entrust his Personal Information to unreasonable security risks, particularly because Mr. Terpin had been subject to the June 11, 2017 hack. In reliance upon AT&T's representations and promises, Mr. Terpin continued to maintain a wireless account with AT&T and to use his AT&T phone number for verification and other promises." Id. ¶ 162.

Mr. Terpin thus clearly alleges "exposure" to statements by AT&T (in this case in a face-to-face meeting with an AT&T representative in which the statements were made), AT&T's intent that Mr. Terpin rely on the representations (by retaining him as an AT&T customer), and the fact that Mr. Terpin in fact did rely on the representations (by continuing to be an AT&T customer). SAC ¶ 92. Thus, even if the Court were to find that Mr. Terpin has not alleged adequate reliance on documents referenced in the SAC, the Fourth Claim for Relief should still proceed on the basis that AT&T made representations to him regarding its security measures

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

after the June 11, 2017 hack on which he relied. *See Johnson v. Riverside Healthcare Sys., LP*, 534 F.3d 1116, 1121-22 (9th Cir. 2008) (to survive a motion to dismiss compliant must present cognizable legal theories and sufficient allegations to support those theories).

2. Mr. Terpin has Adequately Alleged that AT&T's statements were known to be false.

AT&T additionally argues that the claim should be dismissed because Mr. Terpin has not adequately alleged that AT&T did not intend to ignore the heightened security protocol and that all Mr. Terpin has alleged is that AT&T did not perform its promise. In making this argument, AT&T—for the first time after two prior rounds of motion practice—claims under Rule 9(b) of the Federal Rules of Civil Procedure that Mr. Terpin's claim is not plead with particularity (without expressly stating that it is doing so).

Mr. Terpin's claims pass muster under Rule 9(b) because AT&T undoubtedly has notice of the "particular misconduct so that [it] can defend against the charge[.]." *Vess v. Ciba-Geigy Corp., USA*, 317 F.3d 1097, 1006 (9th Cir. 2003). AT&T has knowledge from the SAC of the representations that were made to Mr. Terpin (regarding six-digit "higher level" security), the date of those representations (June 13, 2017), the location (a Puerto Rico AT&T store), and the statements made by the AT&T representative at that meeting. *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007).

Defendant's claim that Mr. Terpin has not adequately alleged that AT&T did not intend to perform its promise can also be expressed as whether AT&T's statements were "false when made." *See UMG Recordings, Inc. v. Global Eagle Entertainment, Inc.*, 117 F. Supp. 3d 1092, 1108 (C.D.Cal. 2015) ("plaintiff must plead facts explaining why the statement was false when made" (quoting *Smith v. Allstate Ins. Co.*, 160 F. Supp. 2d 1150, 1152 (S.D. Cal. 2001)). At the pleading stage of a promissory fraud claim, the determination of this question only "requires

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

pleading facts from which it can be inferred that the promisor had no intention of performing at the time the promise was made." *Id*.

Mr. Terpin here alleges more than mere non-performance. He alleges that AT&T "did not intend to perform either its promises in the Privacy Policy or after the June 11, 2017 hack regarding the security protection that would be given to Mr. Terpin's personal information by adding a six-digit security code on the account." SAC ¶159. The reason why AT&T did not intend to perform its promises was because AT&T "knew that is security protections, including the six-digit security code were ineffectual and could easily be evaded or bypassed by its employees." SAC ¶ 160. Mr. Terpin also alleges that such "representations and promises were . . . false because AT&T was using outdated security procedures and failed to disclose that it did not adhere to its own standards. . . ." *Id.* AT&T further knew that the statements were false because it knew "it did not have in place state-of-the art security protections, such as a SIM lock out." *Id*.

As in *Tenzer v. Superscope, Inc.*, 39 Cal. 3d 18, 30-31 (1985), AT&T's fraudulent intent can be inferred by the facts and circumstances alleged in the SAC, including its knowledge that its employees could easily evade the protections (as shown in statements by an AT&T employee in the *Motherboard* article). Under these circumstances Mr. Terpin has properly alleged that AT&T knew that its promise that such a security standard would protect Mr. Terpin was false when made.[4]

Moreover, Mr. Terpin is not alleging that AT&T failed to "guarantee" security, that its promises were "overly optimistic," or that AT&T had an "honest

[4] The standard for false representations is that they are "false" when made. Falsity can be expressed as the falsity of the statements themselves. *See Smith v. Allstate Ins. Co.*, 160 F. Supp. 2d 1150, 1153-54 (S.D.Cal. 2001), *cited* in the Motion p. 12 (plaintiff must "plead facts explaining why the statement was false when it was made"). In this case, AT&T's statements regarding the security procedures were false not simply because AT&T did not keep its promises, but also because the statements themselves were intrinsically false.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

but unreasonable intent to perform." Motion, p. 13. Instead, Mr. Terpin is alleging that AT&T promoted a security protocol that afforded no real security because it knew that it could be evaded or overridden by its employees. AT&T knew that even after AT&T placed the six-digit code on Mr. Terpin's account that this would not prevent employees from overriding or ignoring the protocol. AT&T's statements to Mr. Terpin after the June 11, 2017 hack were thus demonstrably false.

C. Mr. Terpin Has Properly Alleged Punitive Damages.

1. Mr. Terpin's Alleges Punitive Damages Based on the Actions of AT&T's Officers and Managing Agents.

AT&T's motion to strike punitive damages distorts the allegations of the SAC. Mr. Terpin's claim for punitive damages arises from the direct actions of AT&T undertaken through its officers and management—not from the actions of a single individual (Jahmil Smith).[5] As the SAC alleges, AT&T consciously and maliciously put in place a system that it knew would not protect the security and privacy of its customers' personal information. As the SAC further alleges, the "higher level" security measures that AT&T urged Mr. Terpin to adopt after the first SIM swap on June 11, 2017 were known to AT&T to be ineffectual because they could readily be bypassed or overridden by AT&T employees. SAC ¶¶ 89-92. AT&T is thus subject to punitive damages not because of the actions of the individual who is believed to have turned over the information, but because its corporate managerial employees knowingly implemented and maintained a system that did not protect the private information and communications of its customers. *See Cruz v. Homebase*, 83 Cal. App. 4th 160, 167 (2000) (award of punitive damages against a corporation rests on proof of malice of corporate leaders (citing Cal. Civ. Code § 3294(b)).

[5] Mr. Terpin has alleged claims for negligent supervision and training and negligent hiring (sixth and seventh claims for relief) that may implicate AT&T's actions in regard to employees (or contractors) like Mr. Smith and his employer Spring Communications. *See* Motion, p. 8, n. 3.

a. AT&T Has Violated Its Obligations Under Law By Allowing Its Employees to Turn Over its Customers' Personal Information.

AT&T was well aware of its obligations to protect its customers' personal information and equally well aware that its security systems were inadequate. AT&T had an obligation under Section 222(a) of the FCA, 47 U.S.C. § 222(a), to protect the confidential information of its customers. SAC ¶¶ 28-34. Under the FCC's CPNI Rules implementing the FCA, AT&T was required to establish measures to prevent the disclosure of CPNI by employees to unauthorized individuals, including presentation of adequate means of identification by customers to AT&T. SAC ¶ 34.

Moreover, the SAC alleges that AT&T and its corporate officers were put on notice regarding its employees' disclosure of its customers' personal information through the April 8, 2015 FCC Consent Decree and were required to remedy the deficiencies in AT&T's security, hiring and training practices. *See* SAC ¶¶ 39-51. In conjunction with a pretexting scam, the FCC fined AT&T a record $25 million for violating Section 222 of the FCA by allowing its employees to hand over to thieves the personal information of almost 280,000 customers. *Id.* ¶ 39. In the consent decree of the same date ("Consent Decree") (which remains in full force and effect), the FCC cited (i) AT&T's lax security practices; (ii) the fact that employees were paid by criminals to hand over AT&T customers' personal sensitive information; (iii) the further fact that AT&T employees readily breached AT&T's security; and (iv) AT&T's failure properly to supervise its employees. *Id.* ¶¶ 40-43.

In the Consent Decree the FCC ordered AT&T to (i) take "every reasonable precaution" to protect customers' data; (ii) imposed obligations on AT&T to properly manage and supervise employees; (iii) required AT&T to designate "a senior corporate manager with the requisite corporate and organization authority to

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

serve as a Compliance Officer; and (iv) required the company to implement a "Compliance Plan" including an "Information Security Program," "Ongoing Monitoring and Improvement," and a "Compliance Review." *Id.* ¶¶ 44-47. The "Information Security Program" required under the Consent Decree specifically required AT&T to implement "*access controls reasonably designed to limit access to Personal Information and CPNI to authorized AT&T employees, agents, and Covered Vendor Employees*." ¶ 48 (emphasis added).

b. AT&T's Corporate Officers Deliberately Perpetuated A Grossly Inadequate Security System.

AT&T and its corporate officers Bill O'Hern, who has been AT&T's Chief Security Officer and headed AT&T's security operations since 2016, and David S. Huntley, AT&T's Executive Vice President & Chief Compliance Officer, are presumptively well aware of AT&T's security system and the requirements of the Consent Decree as pertains to employees protecting customers' personal information. SAC ¶ 75. Indeed, Mr. Huntley (who bears the "Compliance Officer" title referenced in the Consent Decree) is responsible at AT&T for "verifying compliance with legal and regulatory requirements of the countries and jurisdictions where AT&T operates, and ensuring adherence to internal compliance standards." *Id.*, citing https://investors.att.com/corporate-governance/leadership. These compliance standards likely include adherence to the requirements of the Consent Decree.

The SAC thus alleges that AT&T deliberately ignored the requirements of the Consent Decree by establishing and continuing to promote to its customers a system that it knew did not protect customers' information. Moreover, AT&T, acting through executives like Messrs. O'Hern and Huntley, did nothing to prevent AT&T employees from turning over that information to hackers in SIM swaps. SAC ¶ 109. The SAC further alleges that AT&T's corporate officers, including Messrs. O'Hern and Huntley, knew that AT&T's security system was inadequate,

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

knew that its employees could readily bypass or ignore the system, and that its employees were susceptible to bribes to turn information over to hackers. SAC ¶¶ 75, 77-79, 83-84, 90-93, 143-45, 149, 156.

Mr. Terpin discovered the manifest deficiencies of the system to his peril when an AT&T employee turned over his information to hackers, despite the vaunted "higher level" security that AT&T had placed on his account. As a result of the disclosure of personal information and communications, Mr. Terpin lost over $24 million in cryptocurrency.

c. The SAC Adequately Alleges that Employees Can Readily Evade or Bypass AT&T's Security System.

Although he has not had the benefit of discovery from AT&T, Mr. Terpin has substantiated his allegations against AT&T with information about other SIM swaps involving AT&T employees and media stories about the security of AT&T and other telecommunications carriers. *See*, *e.g.*, SAC ¶¶ 73-74 (REACT task force cites store employees' involvement in SIM swaps because of carriers' inadequate security); ¶ 76 (carriers are "weakest link" in security according to authors of article in *bitcoinist.com*); ¶78 (*Motherboard* article quotes AT&T employee as stating that AT&T doesn't have sufficient safeguards to stop employees and that the AT&T "system is designed so that some employees have the ability to override security features such as the phone passcode that AT&T (and other companies) now require when porting numbers").

The pattern that emerges from these reports is similar to the pretexting cases that led to the FCC's Consent Decree. As reported by both insiders and law enforcement, AT&T employees are readily bribed to turn over the personal information of its customers to hackers, who use that information to commit SIM swaps. SAC ¶¶ 9, 67, 73. Ignoring the Consent Decree (and apparently not deterred by a $25 million fine), AT&T and its corporate officers are again maintaining a system that does nothing to prevent employees from turning over its

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

customers' personal information and communications. Moreover, as the SAC alleges, AT&T and its officers and managers have not put in place measures, such as a SIM lockdown, that would provide further protection of its customers' information and communications. SAC ¶¶ 14, 143.

2. Cases Involving the Ratification of the Actions of Low-Level Employees are Not Relevant.

Unlike many of the cases cited by AT&T, this is not a case where corporate officers' knowledge of a specific lower level employee charged with wrongful conduct (such as sexual harassment or stalking) provides a basis for punitive damages through ratification of the employee's actions. Instead, the gravamen of Mr. Terpin's allegations is that the actions of AT&T's corporate officers and managing agents were malicious, oppressive and fraudulent.

Under Civil Code § 3294(a), "[i]n an action for the breach of an obligation not arising from contract, where it is proven by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice, the plaintiff, in addition to the actual damages, may recover damages for the sake of example and by way of punishing the defendant."

Civil Code § 3294(b) further provides that "[a]n employer shall not be liable for damages pursuant to subdivision (a), based upon acts of an employee of the employer, unless the employer had advance knowledge of the unfitness of the employee and employed him or her with a conscious disregard of the rights or safety of others or authorized or ratified the wrongful conduct for which the damages are awarded or was personally guilty of oppression, fraud, or malice. With respect to a corporate employer, the advance knowledge and conscious disregard, authorization, ratification or act of oppression, fraud, or malice must be on the part of an officer, director, or managing agent of the corporation."

In order to impose punitive damages on a corporation, California's "punitive damages statute requires proof of malice among corporate leaders: the 'officer[s],

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

director[s], or managing agent[s].'" *Cruz*, at 166. "Managing agents" are "employees who 'exercise [] substantial discretionary authority over decisions that ultimately determine corporate policy.'" *Id*., quoting *White v. Ultramar*, 21 Cal. 4th 563, 577 (1999). The purpose of punitive damages is to punish malice "among corporate leaders" who "guide corporate conduct" and to "avoid[] punishing the corporation for malice of low-level employees which does not reflect the corporate 'state of mind' or the intentions of corporate leaders." *Cruz*, 83 Cal. App. 4th at 167.

Many of the cases cited by AT&T are irrelevant to the allegations of the SAC because they involve the issue of whether a corporation through its managing agents ratified the conduct of a lower level employee. For example, in *Weeks v. Baker & McKenzie*, 63 Cal. App. 4th 1128, 1154 (1998) the issue was whether a law firm was liable for the actions of an employee because an "officer, director or managing agent" had knowledge of the unfitness of the employee and employed him with the conscious disregard of the safety of others. *See* Motion, p. 15. Similarly, in *Coll. Hosp. Inc. v. Superior Ct.*, 8 Cal. 4th 704, 726 (1999) the issue related to an employer's ratification of an employee's misconduct. *See also Razo v. TIMEC Co.,Inc.*, 2017 WL 5079249, at *19 (N.D.Cal. Nov 3, 2017) (lack of knowledge of executives of an unfit employee. These cases (and similar cases cited by AT&T) are not applicable here because Mr. Terpin is alleging that AT&T directly engaged in despicable conduct by setting "corporate policy" through its officers, directors and managing agents, not that it ratified the actions of Jahmil Smith. *See Cruz*, *supra*, at 167-168.

Contrary to AT&T's implication, Mr. Terpin did not pull the names of Mr. O'Hern and Mr. Huntley out of a hat. Based on publicly available information, these are precisely the individuals at AT&T who are responsible for setting AT&T's corporate policy regarding security and privacy matters. SAC ¶¶ 75, 77-79, 83-84, 90-93, 143-45, 149, 156. Although Mr. Terpin has not had the benefit of

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

discovery to uncover the exact mechanics of AT&T's implementation of its ineffective security program, Mr. Huntley is the Chief Compliance Officer of AT&T (and thus was called upon in the FCC's Consent Decree to implement improvements to AT&T's security system necessary to prevent its employees from turning over the personal information of its customers). According to publicly available information, Mr. Huntley is also responsible for regulatory compliance and privacy at AT&T. *See* SAC ¶ 75, *citing* https://investors.att.com/corporate-governance/leadership (article on David S. Huntley). Mr. O'Hern is also named because he is in charge of security at AT&T and is thus charged with making sure that customers' information is secure. SAC ¶ 75, *citing* https://about.att.com/innovationblog/030116billohern (article on Bill O'Hern). In any event, AT&T's assertions on this issue are not properly addressed at the pleading stage.

3. Mr. Terpin Has Adequately Alleged Malice, Oppression and Fraud by AT&T and its Managing Agents.

AT&T further argues that Mr. Terpin has not plead the requisite mental state of its officers and managing agents. This argument rests on the same misconception as its first argument, *i.e.*, that the requisite mental state relates to such officers' knowledge regarding a single individual (Mr. Smith) as opposed to the mental state of the executives and managing agents themselves as to AT&T's inadequate security program. In that regard, Mr. Terpin has indeed specifically alleged facts, including "conduct that is both willful and despicable" and that "subjects a person to cruel and unjust hardship in conscious disregard of that person's rights." Motion, p. 19, quoting *Lackner v. North*, 135 Cal. App. 4th 1188, 1211, 1213 (2006); *Perez v. Auto Tech. Co.*, 2014 WL 12588644 (C.D.Cal. July 14, 2014). *See also* Cal. Civ. Code § 3294(c)(1) (defining malice (in part) as "conduct which is carried on by the defendant with a willful and conscious disregard of the rights of others"); § 3294(c)(2) (defining oppression as "despicable conduct that

subjects a person to cruel and unjust hardship in conscious disregard of that person's rights") and § 3294(c)(3) (defining fraud as "intentional misrepresentation, deceit or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury").

Mr. Terpin alleges that AT&T, despite its knowledge that its employees had betrayed the privacy of customer accounts previously and its obligation under the Consent Decree to institute a security program that would prevent its employees from turning over customer information to third parties, consciously and deliberately established a security system that it knew could be overridden or ignored by employees to turn over customer information to hackers for SIM swaps. The SAC further alleges that AT&T did not properly hire, monitor or supervise its employees (despite its obligation to do so under the Consent Decree). Moreover, AT&T consciously and deliberately violated the promises that it made in its privacy policies about protecting customers' information by encouraging Mr. Terpin after the June 11, 2017 SIM swap to implement a six-digit code that it knew could easily be evaded or overridden by its employees. These allegations are substantiated by statements by law enforcement and an AT&T employee. SAC ¶¶ 73-74, 77-78. These actions are not only malicious and oppressive, but also constitute fraud. Indeed, Mr. Terpin in his third and fourth claims for relief allege the elements of both claims for misrepresentation and false promise involving the acts of AT&T officers and managing agents. Such actions undoubtedly are fraud under Civil Code § 3294(c)(3).

AT&T is incorrect that the SAC merely contains "conclusory allegations." As outlined above, the SAC contains detailed allegations replete with context and citations to other sources substantiating a pattern on the part of AT&T and its employees. Contrary to AT&T's unsupported charge, the inferences that Mr. O'Hern and Mr. Huntley were knowledgeable and were involved in the corporate

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

policy is established by their roles in the company as stated in AT&T's public materials. Indeed, Mr. Huntley as AT&T's "Compliance Officer" is charged with protecting customers' personal information. *See* SAC ¶¶ 46, 56 and 75. Because of their roles and responsibilities, Messrs. O'Hern and Huntley are charged with knowledge of the security lapses that led employees to divulge personal information to third parties to facilitate SIM swaps and AT&T's obligations to comply with its responsibilities to protect customers' personal information.

4. Mr. Terpin may Obtain Punitive Damages for Claims 5-7.

AT&T further alleges that punitive damages are not available for Mr. Terpin's claims for negligence, negligence supervision, and negligent hiring. AT&T cites no authority for striking the punitive damages for these claims at this stage prior to discovery. The unremarkable principle that punitive damages may not be based on mere negligence is a principle that applies to an award of punitive damages *at trial*—not striking the claims at the pleading stage before discovery has even commenced.

As the SAC alleges, the Consent Decree called upon AT&T to remediate its hiring, training and retention policies of employees to prevent employees turning over customers' personal information to unauthorized third parties. SAC ¶¶ 40-51. If it is shown at trial that AT&T's officers and other managing agents knew that it continued to engage in defective hiring, training and retention policies and that such actions were undertaken with malice, fraud or oppression (as alleged in the SAC), Mr. Terpin may be entitled to punitive damages for these claims, as well as the claims alleging fraud. This, however, is a matter not for a motion to dismiss, because it involves factual issues.

5. This is Not a Case of First Impression.

The fact that this case involves SIM swapping (instead some other form of a security breach) is not a ground for dismissing the prayer for punitive damages at the pleading stage. Although the facts of this case (as with many other cases) may

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

involve some unique elements, the legal issues are not unique, i.e., AT&T's liability for actions that it undertook that exposed Mr. Terpin's personal information in violation of his rights.

The rationale for the rule that punitive damages may not be appropriate in cases of first impression is that "the requisite intent or willfulness required to consciously disregard another's rights cannot be present if no right or duty has been recognized." *In re First Alliance*, 2003 WL 21430096, at *10 (C.D.Cal. June 16, 2003). Because punitive damages must be based on conscious disregard of another's rights, the Ninth Circuit in a "close case" found that they were not appropriate where there not a clear tenable claim of right. *Morgan Guar. Trust Co. v. American Sav. & Loan Ass'n*, 804 F.2d 1487, 1500 (9th Cir. 1986).

In contrast, the rights at issue in this case are well established and recognized. Mr. Terpin as an AT&T customer had a statutory right for protection of his personal information and communications under the FCA and AT&T had the obligation to protect that information. SAC ¶¶ 28-32. Indeed, the FCA gives Mr. Terpin a private right of action to enforce those rights under the FCA and he is seeking to do so in this action. SAC ¶¶ 133-141. Mr. Terpin's rights are further based on the CPNI Rules that require carriers like AT&T to implement measures to prevent disclosure of personal information to unauthorized individuals. SAC ¶¶ 32-34. Moreover, the FCC enforced consumers' rights to the privacy of personal information against AT&T in the pretexting cases and through the resulting Consent Decree. In those cases, as here, AT&T inadequately protected its customers' personal information from being turned over to criminals by its employees. SAC ¶¶ 35-51. AT&T itself acknowledges these rights in its Privacy Policy and Code of Business Conduct. SAC ¶ 52 *et seq.* For example, in its Privacy Policy, AT&T states that it takes its responsibility to safeguard customers' personal information "seriously" and that it will not share such information except for legitimate business purposes. *Id.* ¶ 54. It also promises that it has safeguards in

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

place to protect such information, including safeguards as to how its employees protect such information. *Id*. ¶ 55.

Under these circumstances, there is nothing novel about the rights at issue in this case. Nor, unfortunately, is there anything novel about the fact that AT&T did not have safeguards in place to protect the security of Mr. Terpin's information from the actions of its own employees, given that it was fined $25 million in 2015 for similar actions. Under the rationale of *In re First All Mortg*., the rights and duties involved here are well-established and can readily serve as a basis for a punitive damages claim based on AT&T's malicious flaunting of those rights in the case of Mr. Terpin.

Moreover, as the foregoing discussion shows, there are—at a minimum—disputed facts as to AT&T's claim that this case is sufficiently "novel" so as to avoid punitive damages that would make it improper to strike these allegations at the pleading stage and without allowing Mr. Terpin the benefit of discovery.

III. CONCLUSION

For the foregoing reasons, the Court should deny Defendant's Motion to Dismiss Third and Fourth Claims for Relief and Mr. Terpin's claim for punitive damages. Alternatively, Mr. Terpin seeks leave to amend such claims.

DATED: April 13, 2020

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By:/s/ Pierce O'Donnell
PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff MICHAEL TERPIN

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590